Pakistan National PKI

Certificate Policy (CP) for Trust Services Providers (TSPs)

Version control

Version	Date	Description / Status	Responsible
V1.0	08/12/2022	Initial version for review & approval	ECAC
V1.1	26/12/2022	Corrected the URLs, Email Addresses, Object IDs	ECAC
V1.2	22/02/2023	Accommodated comments by ECAC Design Authority	ECAC
V2.0	22/11/2024	Updated to accommodate the changes in the PKI hierarchy after ECAC's intermediate CAs /NTC CAs termination.	ECAC

Document Signoff

Version	Date	Responsible	Validated By	Reviewed and Approved By
V2.0	/ /2024	ECAC	ECAC (PMA)	ECAC (PMA)

Table of Contents

1 Introduction

The present document is the Certificate Policy (hereinafter, the CP) indorsing requirements applicable to the provision of certification services offered by the Trust Services Providers (TSP) issuing publicly trusted certificates to end-entities in Pakistan.

Trust Services Providers are established and operated in Pakistan under the Pakistan national PKI accreditation framework and the applicable laws in Pakistan. The ECAC is mandated to operate the national PKI accreditation framework and hence it is responsible for authorizing TSPs offering certification services in Pakistan.

This CP addresses the technical, procedural, and organizational policies of the CAs operated by the TSPs with regard to the complete lifetime of certificates issued by these CAs.

The provisions of the present CP regarding practices, level of services, responsibilities and liability bind TSPs, its CAs, subscribers and relying parties.

This CP complies with the formal requirements of the Internet Engineering Task Force (IETF) RFC 3647 with regards to format and content. While certain section titles are included according to the structure of RFC 3647, the topic may not necessarily apply in the implementation of the TSPs' CAs. Such sections are denoted as "Not applicable". Additional information is presented in subsections of the standard structure where required.

The CP complies with the Electronic Transaction Ordinance 2002 (ETO 2002) of Pakistan for Digital Signature and Electronic Certification and ECAC Regulations formulated under ETO 2002.

This CP complies with the below requirements published at https://www.cpacanada.ca :

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities - SSL Baseline
- WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL
- WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements
- WebTrust Principles and Criteria for Certification Authorities – Network Security
- WebTrust Principles and Criteria for Certification Authorities – S/MIME

The ECAC's Policy Management Authority (PMA) is committed to maintain this CP in conformance with the current versions of the requirements below published at http://www.cabforum.org :

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates
- CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates

- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates

If there is any inconsistency between this document and the requirements above, the above requirements take precedence over this document.

Further information with regard to this CP can be obtained from the ECAC PMA, using contact information provided in clause 1.5.

1.1 Overview

The Pakistan National PKI aims to provide digital certification and trust services to government and commercial sectors, enabling individuals and entities within Pakistan to conduct secure electronic transactions.

In this framework, ECAC operates as a trust service provider, delivering trust services to the government sector via a structured hierarchy of Certification Authorities (CAs). Furthermore, ECAC establishes a foundation for additional trust service providers that support both the commercial & Government sectors.

This setup provides a resilient framework to support variance in requirements between government and non-government sectors regarding the offering and consumption of certification and other trust services.

The Pakistan National PKI comprises a CA hierarchy of two (2) levels:

1. **Level 1:** The CAs at this level are positioned at the top of the hierarchy, serving as the trust anchor for Pakistan's National PKI. This level comprises five offline, self-certified CAs responsible for certifying the next layer of Certification Authorities. Root CAs are:
    a. ***Code Signing Root CA:*** Root CA to certify/sign Code Signing Subordinate CAs,
    b. ***S/MIME Root CA:*** Root CA to certify email protection Subordinate CAs.
    c. ***TLS Root CA:*** Root CA to certify SSL/TLS Subordinate CAs.
    d. ***Client Auth Root CA:*** Root CA to certify Client Auth Subordinate CAs.
    e. ***Timestamp Root CA:*** Root CA to certify TSA Subordinate CA

2. **Level 2:** This level includes ECAC's Subordinate CAs dedicated to serving the government sector, each certified by the corresponding Root CA at the top (Level 1) of the hierarchy.

    Additionally, Subordinate CAs operated by authorized (i.e., licensed) Trust Service Providers (TSPs) for delivering trust services to the commercial and governement sectors are also part of this level. These Subordinate CAs will be technically constrained through a combination of Extended Key Usage and, optionally, Name

Constraint extensions to restrict the scope within which TSPs may issue end-user certificates.

The licensing process is addressed to TSPs that meets the contractual, audit and policy requirements of ECAC root services with regard to operational practices and technical implementation.

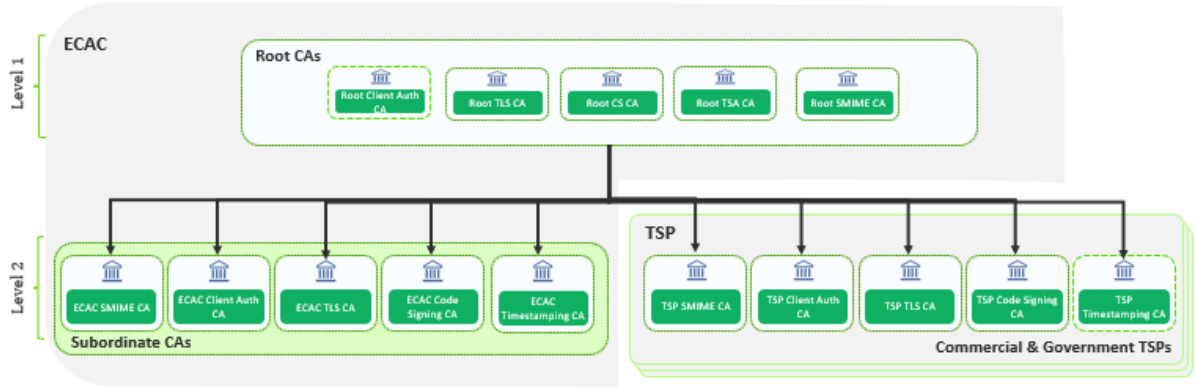

Figure 1 - Pakistan national PKI hierarchy

1.2 Document Name and Identification

This document is the "Certificate Policy (CP) for Trust Services Providers (TSPs)" by the ECAC Pakistan, and it was approved by the ECAC Policy Management Authority (PMA) for the publication.

This CP document is published at https://ecac.pki.gov.pk

The OID **1.3.6.1.4.1.59337.2.1** is used to identify this document.

TSPs shall include the above mentioned OID in the CP extension of their CAs to indicate compliance with the present CP. TSPs shall represent, in its applicable CPS, that all certificates containing the above OID indicating compliance with this CP and are issued and managed in accordance with this CP.

1.3 PKI Participants

Several parties make up the participants of a TSP Subordinate CA, including:

- Subordinate CA,
- Registration Authorities (RA) used by the TSP to register end-entities to which end-entity certificates are issued,
- Subscribers,
- Relying parties.

These participants, collectively called PKI participants, and their roles are described in the following sections.

1.3.1 Certification Authorities

Subordinate CAs

Subordinate CAs are operated by Trust Service Providers (TSPs) based in Pakistan and are approved for inclusion in the PKI domain—either the Governmental PKI domain or the Commercial PKI domain—according to the Pakistan National PKI Accreditation Framework. Each Subordinate CA is certified by the respective Root CAs, as listed in Section 1.1.

The Subordinate CAs shall be operated in accordance with a Certification Practice Statement (CPS) that is defined by the TSP in compliance with the present CP.

The Subordinate CAs are technically constrained to restrict the issuance of digital certificates through constraints such as length of certification paths, extended key usage, name constraints, and inclusion of certificate policy OIDs.

TSPs shall undergo an independent WebTrust audit and timely present the unqualified WebTrust assurance reports to ECAC, in addition to complying with the national accreditation framework endorsed by the ECAC.

1.3.2 Registration Authorities

The TSP shall set up or delegate the RA function according to this CP. The RA function consists of Registration Authority Officer (RAO), operators, products, systems, and procedures used by the Subordinate CA to validate the identity of subscribers requesting the issuance of certificates.

The personnel involved in the RA function shall meet and follow the requirements set forth in Sections 4.2 and 5.3.

In the case of delegating the RA function to a third-party organization that may offer this service by law, the TSP remains fully responsible and accountable for the operations performed by the delegated RA.

Before the TSP authorizes a Delegated Third Party to perform a delegated RA function, the TSP SHALL contractually require the delegated third party to:

1. Meet the qualification requirements of Section 5.3.1, when applicable, to the delegated function.
2. Retain documentation in accordance with Section 5.5.2.
3. Comply with this TSP CP
4. Undergo a WebTrust Audit for the delegated RAs (it's required to present a nonqualified WebTrust reports to TSP on time).

The TSP may authorize an organization to have their own Enterprise RA to authorizes issuance of Certificates to that organization. The TSP's annual audit shall also include the audit of the Enterprise RA function.

The TSP SHALL verify that the Enterprise RA and Delegated Third Party involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3

1.3.3 Subscribers

A TSP's Subscriber is any natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use .

1.3.4 Relying Parties

Relying parties are any natural or legal person that relies on a valid certificate and / or a digital signature verifiable with reference to a public key listed in a subscriber's certificate

1.3.5 Other Participants

Other Participants include:

- The ECAC PMA is the supervision authority responsible for supervising the entire activity of the licensed TSP. The roles and responsibilities of PMA are described in its Root CP/CPS published at: https://ecac.pki.gov.pk.
- Qualified independent WebTrust auditors who verify the requirements set out in section 8.2.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

This CP defines a range of distinct certificate types that can be supported by Subordinate CAs. The different types have different intended uses, such as:

- Electronic Signature / eSeal: for producing digital signatures on digital transactions and documents.
- S/MIME: for email Signing and encryption.
- Code Signing and EV Code Signing: for producing digital signatures for applications, drivers, executables, and software programs.
- OV SSL certificates: Used to secure online communication with a moderate level of trust, suitable for business websites and portals.
- EV SSL certificate: Used to secure online communication with the highest level of trust, making it ideal for banking, e-commerce, and other sites handling sensitive transactions.
- Secure Timestamps: for applications where the proof of a particular action or fact must be guaranteed with the exact time source.

The Subordinate CA shall restrict the use of certificates it issues using appropriate certificate extensions with regards to key usage and extended key usage, which shall be configured according to the certificate type.

The TSP's CPS shall specify, in accordance with the present CP, and particularly its section 7, the appropriate certificate usage that applies to each type of certificate it issues,

1.4.2 Prohibited Certificate Uses

The TSP CPS shall specify the certificate usage restrictions that apply to each type of certificate it issues. Any usage of the certificate inconsistent with these restrictions, with the appropriate usage or with the contents of this CP and TSP CPS shall not be authorized.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP document is administered by the ECAC PMA.

1.5.2 Contact Person

Information requests or inquiries related to the present document will only be accepted if addressed to the PMA at:

Policy Management Authority
Electronic Certification Accreditation Council (ECAC),
5th Floor NTC HQ Building, G-5/2,
Islamabad, Pakistan
Tel: +92 51 9245739
Email: ecac.certification.info@pki.gov.pk

The ECAC PMA accepts comments regarding the present document only when they are addressed to the contact above.

1.5.3 Person Determining CPS Suitability for the Policy

The TSP is responsible for ensuring that its CPS conforms to this CP.

The final decision on confirmation of suitability rests with the ITPC PMA, based on information supplied by the TSP PKI GB. This process may be supported by an audit report from an auditor as supported in the national accreditation framework

1.5.4 CPS Approval Procedures

This CP is subject to approval by the ITPC PMA. The Process entails reviewing the initial draft of this CP and any subsequent modifications by the PMA's specialist staff (i.e. PMA members) to determine consistency with implemented best practice. The modifications may take the form of a document containing a modified version of the CP, or an update notice. Changes made into this CP will be tracked in the revision table.

The PMA communicates with the TSP PKI GBs in relation to amendments to this CP and formally approves the newer versions.

On an annual basis, if no other changes are made to this CP, its version number is incremented, and a dated changelog entry is added to denote that.

1.6 Definitions and Acronyms

1.6.1 Definitions

The following is a list of the definitions of terms and acronyms used. The source is cited where relevant.

Advanced certificate: As per the Pakistan National PKI context, the advanced certificate is a form of digital certificate issued after conducting a moderate verification of the subject's identity. It is utilized for generating a moderate (advanced) digital signature on electronic documents and transactions.

Applicant – The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber.

Applicant Representative – A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA. In the context of this CP, the applicant representative is in charge of submitting certificate requests and certificate revocation requests on behalf of the applicant.

Activation data – Secret information, other than cryptographic keys, that are required to operate cryptographic modules that need to be protected, e.g. a PIN, a password or passphrase, or a manually held key share.

Attestation Letter – A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information. In the context of this CP, attestation letters are signed by Human Resource teams of government entities.

Audit Period – In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA)

CA Key Pair – A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

Certificate – An electronic document that uses a digital signature to bind a public key and an identity

Certificate Data - Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process - Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates

Certificate Policy (CP) – A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report – Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List – A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority – An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement – One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Certificate Profile – A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g., a Section in a CA's CPS or a certificate template file used by CA software.

Control – "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country – Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

CSPRNG – A random number generator intended for use in cryptographic system.

Expiry Date – The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

EV Certificate – A certificate that contains subject information specified in these Guidelines and that has been validated in accordance with the EV Guidelines.

EV Certificate Request – A request from an Applicant to the CA requesting that the CA issue an EV Certificate to the Applicant, which request is validly authorized by the Applicant and signed by the Applicant Representative.

HSM – Hardware Security Module – a device designed to provide cryptographic functions specific to the safekeeping of private keys

IP Address – A 32-bit or 128-bit label assigned to a device that uses the Internet Protocol for communication.

Issuing CA – Issuing CAs are used to provide certificates to users, computers, and other services. In this CP, Issuing CA is issued by a Subordinate CA, and it issues certificates to the end entities only.

Key Compromise – A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.

Key Generation Script – A documented plan of procedures for the generation of a CA Key Pair.

Key Pair – The Private Key and its associated Public Key.

Legal Entity – An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Object Identifier – A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder – An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol – An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Private Key – The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key – The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure – A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly Trusted Certificate – A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor – A natural person or Legal Entity that meets the requirements of Section 8.2.

Qualified certificate: As per the Pakistan National PKI context, the qualified certificate is a type of digital certificate issued following a thorough verification of the subject's identity with a high degree of assurance. This verification process typically involves a face-to-face meeting or equivalent methods that provide a comparable level of reliability. Qualified certificates are utilized for generating qualified digital signatures on electronic documents and transactions.

Registration Authority (RA) – Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Relying Party – Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository – An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Root CA – The top-level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate – The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Subject – The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information – Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA – A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber – A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Subscriber Agreement – An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use – Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Baseline Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Top-level Domain: A top-level domain is the last part of the text in a domain name like .com, .net or .org

Valid Certificate – A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialists: Someone who performs the information verification duties as specified in this CP.

Validity Period – The period of time from notBefore through notAfter, inclusive.

1.6.2 Acronyms

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CCTV	Closed Circuit TV
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CV	Curriculum Vitae
DN	Distinguished Name
ECAC	Electronic Certification Accreditation Council
EV	Extended Validation
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
ISO	International Standards Organization
NTC	National Telecom Corporation
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Information Number
PKCS#10	Certification Request Syntax Specification
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RSA	Rivest-Shamir-Adleman
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SSL	Secure Sockets Layer
TSA	Timestamping Authority
TLS	Transport Layer Security

TSP	Trust Service Provider
UPS	Uninterruptible Power Supply
URI	Universal Resource Identifier, a URL, FTP address, email address, etc.
URL	Universal Resource Locator
VPN	Virtual Private Network

1.6.3 References

This document refers to the following:

- X.509 - The standard of the ITU-T (International Telecommunications Union-T) for Certificates.
- RFC3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- AICPA/CPA Canada WebTrust for Certification Authorities Principles and Criteria
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities - SSL Baseline
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Network Security
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – S/MIME
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates
- CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
- Electronic Transaction Ordinance 2002 of Pakistan for Digital Signature and Electronic Certification

2 Publication and Repository Responsibilities

2.1 Repositories

The TSP shall publish and maintain applicable CPS(s), relevant policies, and agreements (ex. subscriber, RA and relying party agreements), Subordinate CA certificates, Subordinate CA OCSP responder certificates, TSA certificates, Subordinate CA CRLs, and the WebTrust audit reports via an online and publicly accessible website (hereinafter, the TSP public repository).

2.2 Publication of Certification Information

The TSP shall publish a copy of the Subordinate CA certificates, TSA certificates, as well as a link to this CP in the TSP public repository.

The TSP shall publish certificate validity status information in frequent intervals as indicated in this CP. The provision of the certificate validity status information shall be 24/7 available service offered as follows:

- CRLs including any changes since the publication of the previous CRL, at regular intervals. The Subordinate CA shall add a pointer (URL) to the relevant CRL in the Subscribers' certificates as part of the CDP extension whenever this extension is present,
- RFC 6960 compliant OCSP responder. The Subordinate CA shall add the OCSP URL in the AIA extension of the Subscribers' certificates.

2.3 Time or Frequency of Publication

Updates of this CP are published within five days of the ITPC PMA approval. Each compliant TSP shall publish their updated CPS(s) in accordance with the latest version of this CP within 30 days of the ITPC PMA approval.

2.3.1 CA Certificates

Subordinate CA and OCSP responder certificates shall be published in the public repository from issuance until they expire or are rekeyed, after which they will be moved to the archive.

2.3.2 CRLs

Subordinate CAs shall maintain and publish CRLs as follows:

- CRLs shall be refreshed no later than every 24 hours, even if no changes have occurred since the last CRL issuance.
- CRLs lifetime shall be set to 26 hours.

Code Signing TimeStamping Subordinate CA shall maintain and publish CRLs as follows:

- The Subordinate CA SHALL update and reissue CRLs at least once every twelve months and
- within 24 hours after revoking a Timestamp Certificate, and the value of the nextUpdate field MUST NOT be more than twelve months beyond the value of the thisUpdate field

2.4 Access Controls on Repositories

The information published in the TSP public repository is publicly available being guaranteed unrestricted access to read.

The TSP shall implement measures regarding logical and physical security to prevent unauthorized persons from adding, erasing, or modifying entries from the repository.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The TSP CAs follow the standard X.500 distinguished names. The names must be unique and meaningful.

The tables below specify the DN structures that the TSP shall follow for each of the support certificate types.

3.1.1.1 For Certificates issued to Legal persons:

eSeal certificate

Attribute	Value
CN	Full organization registered name
OrganizationID	An identification of the subject organization different from the organization name
O	Organization's legal name
Country – "C"	PK

Code signing Certificate

Attribute	Value
CN	Full organization registered name
O	organization's legal name
Country – "C"	PK
L (optional if S is present, otherwise mandatory)	name of the locality where the organization is established
S (optional if L is present, otherwise mandatory)	the province where the organization is established

EV Code signing Certificate

Attribute	Value
CN	Full organization registered name
O	organization's legal name
BusinessCategory	subject business category[1] as defined in CS BR.
jurisdictionCountryName	Country information MUST be specified using the applicable ISO country code
jurisdictionLocalityName (Optional)	MUST be specified using the full name of the applicable jurisdiction.
jurisdictionStateOrProvinceName (Optional)	MUST be specified using the full name of the applicable jurisdiction.

[1] The organization's business category MUST contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon whether the Subject qualifies under the terms of Section 4.1.1.1," Section 4.1.1.2, Section 4.1.1.3 or Section 4.1.1.4 of the CS BR.

serialNumber	Registration number or where applicable date of registration as defined in CS BR.[2]
Country – "C"	PK
L (optional if S is present, otherwise mandatory)	name of the locality where the organization is established
S (optional if L is present, otherwise mandatory)	the province where the organization is established

Organization Validation (OV) SSL/TLS Certificate

Attribute	Value
subjectAltName	public IP or FQDNs or authenticated domains that are under the control of the Subscriber
CN (Optional)	FQDN(s) or public IP address, potentially linked to the subjectAltName
O	full registered name of organization to which the certificate is issued
Country – "C"	PK
L (optional if S is present, otherwise mandatory)	name of the locality where the organization is established
S (optional if L is present, otherwise mandatory)	the province where the organization is established

Extended Validation (EV) TLS/SSL certificates:

Attribute	Value
subjectAltName	A Fully-Qualified Domain Name. No Wildcard Domain Name is allowed
CN (Optional)	FQDN(s) potentially linked to the subjectAltName
O	full registered name of organization to which the certificate is issued
businessCategory	subject business category[3] as defined in EV guideline
jurisdictionCountryName	Country information MUST be specified using the applicable ISO country code
jurisdictionLocalityName (Optional)	MUST be specified using the full name of the applicable jurisdiction.

[2] For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.

[3] contains one of the following strings: "Private Organization», «Government Entity", "Business Entity", or "Non-Commercial Entity"

jurisdictionStateOrProvinceName (Optional)	MUST be specified using the full name of the applicable jurisdiction.
serialNumber	Registration number or where applicable date of registration
Country – "C"	PK
L (optional if S is present, otherwise mandatory)	name of the locality where the organization is established
S (optional if L is present, otherwise mandatory)	the province where the organization is established

3.1.1.2 For Certificates issued to Natural persons:

Attribute	Value
GivenName	Individual's authenticated given name
SurName	Individual's authenticated surname
SERIALNUMBER	unique identifier for each individual as constructed by the RA
CN	concatenation of given name and surname separated by a "space" character
O (optional)	organization name of a legal entity associated with the natural person
L (optional if S is present, otherwise mandatory)	person's locality name
S (optional if L is present, otherwise mandatory)	the state/province that the person belongs to
Country – "C"	PK

3.1.1.3 Device authentication certificates:

Attribute	Value
CN	system unique common name, unique device identifier or IP address that are applicable
O	organization's legal name
L (optional if S is present, otherwise mandatory)	organization's locality name
S (optional if L is present, otherwise mandatory)	the state/province that the organization belongs to
Country – "C"	PK

3.1.1.4 TSA and OCSP responder certificates

TSA service certificate

Attribute	Value
CN	Service common name
OrganizationID	An identification of the organization different from the organization name
O	full registered name of organization to which the certificate is issued
Country – "C"	PK

OCSP responder certificate

Attribute	Value
CN	The full registered name of the subject
O	A name commonly used by the subject to represent itself
Country – "C"	PK

3.1.2 Need for Names to be Meaningful

All end-entity certificates issued by the TSP CA shall be meaningful and shall uniquely identify the subject.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous or pseudonymous subscribers are not permitted.

3.1.4 Rules for Interpreting Various Name Forms

The naming convention used by the TSP CA shall be based on ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.5 Uniqueness of Names

The TSP shall enforce the controls that are necessary to guarantee that subject Distinguished Names (DN) are unique. Minimum controls enforced:

- For certificates issued to natural and legal persons, the TSP shall enforce a convention for a meaningful representation uniquely identifying the person.
- Certificates issued to devices shall uniquely identify the device. Options include using the registered public DNS name or public IP addresses.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants SHALL NOT use names in their Certificate Application or Certificate Request that infringes upon the intellectual property rights of organizations outside of their authority.

Names can only contain trademarks in case the subscriber has the legal right to use the trademark in question.

For EV Certificates, TSPs shall not allow including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific person or Legal Entity unless it has verified in accordance with the Identity Validation requirements of this document, the EV Guidelines, and the CS BR.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The TSP RA shall validate the proof of possession of private key by subscribers

3.2.2 Authentication of Organization Identity

3.2.2.1 Identity

The TSP RA shall validate the identity and related information of the organization through a reliable authoritative source that allows the verification of the organization's presence, legal name, authorized representatives, and address. Such sources could be:

- for Government entities: the *Official* Government *Gateway*, and
- for non-Government entities: *"Securities and Exchange Commission of Pakistan" or "Federation of Pakistan Chambers of Commerce & Industry"*

Organization identity validation requirements can be summarized as follows:

1. Verification of presence and legal standing:
   1.1. Verify the existence of the Organization using an authoritative source that provides information on the formation of organization including its legal name, address and a reference of the decree or law issued to establish the organization under its designated name. The TSP RA shall also conduct a site visit to the organization's site to validate the address unless there are other trusted means of verifying the organization's address, that shall be approved by the ECAC PMA.
   1.2. Verify the organization's authorized representative approving the certification request. This can be established either based on the organization's record at the authoritative source or an approved a formal communication between the TSP and the organization, the type and requirements of such communication need to be approved by the ECAC PMA.
2. Verification of association with the certificate subject: The TSP RA shall verify that the organization name to be inserted in the certificate matches the legal name of the organization requesting the certificate. The full organization's name of an abbreviated version can be included in the certificate.

For EV TLS & EV Code Signing certificates, TSPs shall conduct additional verifications related to legal, physical and operational existence of the organization according to the EV guidelines and CS BR.

3.2.2.2 Validation of Domain name

For SSL/TLS certificates, the control or ownership of the domain name(s) /IP address which is/are specified in the certificate application shall be verified in accordance with section 3.2.2.4 & 3.2.2.5 of the SSL BR.

3.2.2.3 Validation of mailbox authorization or control

Control or ownership of the domain portion of email addresses shall be verified before the issuance of S/MIME certificates in accordance with section 3.2.2 of the BR for S/MIME. The TSP SHALL NOT delegate the verification of mailbox authorization or control.

3.2.3 Authentication of Individual Identity

3.2.3.1 Tools and mechanisms for Authentication of Individual Identity

This section defines tools and types of mechanisms that can be used for identification and authentication of an individual's identity.

3.2.3.1.1 Types of evidences:

Primary Evidences:

Primary evidence is issued by an authoritative source and is hence trusted regarding the identity attributes the evidence conveys. The accepted evidence is a secure government-issued ID card or passport which is issued with robust identity proofing, issuance, and management processes.

Secondary Evidences:

Evidence that is used in addition to the authoritative evidence to strengthen the reliability of the identity proofing, and as evidence for attributes that are not evidenced from the authoritative evidence (i.e., trusted registers, proof of access, official document and attestations etc.).

3.2.3.1.2 Authoritative source

An authoritative source is any source, irrespective of its form, that is nationally trusted to provide valid and accurate data, information and/or evidence that can be used to prove the identity of an individual. A source may only be authoritative for the data provided by it.

It is important to ensure that the information claimed to be provided by a claimed authoritative source is authentic, i.e., that it originates from a known authoritative source, is genuine and its integrity has been verified.

Examples of authoritative sources can include:

- physical identity document,
- digital identity document,
- eID means used in an authentication protocol, or
- digital signature supported by certificate.

3.2.3.2 Identity validation requirements

Certificate type	Identity validation requirements

• Natural person certificates for **Advanced**[4] electronic signatures • Natural person certificates for authentication	**The TSP shall verify the applicant's identity lawfulness as follows**: **Minimum Personal information to be collected:** • full name (including surname and given names), • date and place of birth, • a serial number or other attributes which may be used to distinguish the person from others with the same name. **Attribute and evidence collection:** The natural person shall be bound to present upon the request of the TSP's Registration Authority the following documents: • Subscriber agreement • Identity Documents (Primary evidence): either Physical Identity or digital Identity (eMRTD) When the subject is a natural person who is identified in association with a legal person (Employee use case).: • Official documents (Secondary evidence) demonstrating that the legal entity acts as the natural person's employer or that there is a legally binding agreement between them. **Attribute and evidence validation:** the TSP shall validate the authenticity of submitted evidence to establish that: - They are valid pieces of evidence - The identity is not that of a deceased person (individual). **The TSP MAY verify the link between the claimed identity and the claimant through the following mechanisms:** • By face-to-face meeting with the applicant or equivalent via one of following methods: o By an attended remote, where the individual communicates in real time with a human registration authority (i.e., RAO). o By Unattended remote, where the communication with the applicant is automated (without involvement of a

[4] Refer to the definition of advanced certificates in section 1.6

	human Registration Officer (i.e., RAO)).
• Natural person certificates for **Qualified**[5] electronic signatures	**The TSP shall verify the applicant's identity lawfulness as follows**: **Minimum Personal information to be collected:** • full name (including surname and given names), • date and place of birth, • a serial number or other attributes which may be used to distinguish the person from others with the same name. • in case of email protection certificate, the applicant' email address is required. **Attribute and evidence collection:** The natural person shall be bound to present upon the request of the TSP's Registration Authority the following documents: • Subscriber agreement • Identity Documents (Primary evidence): either Physical Identity or digital Identity (eMRTD) When the subject is a natural person who is identified in association with a legal person (Employee use case): • Official documents (Secondary evidence) demonstrating that the legal entity acts as the natural person's employer or that there is a legally binding agreement between them. **Attribute and evidence validation:** the TSP shall validate the authenticity of submitted evidence to establish that: - They are valid pieces of evidence - The identity is not that of a deceased person. **The TSP shall verify the link between the claimed identity and the claimant through the following mechanisms:** • By face-to-face meeting with the applicant or equivalent via one of following methods: o By an attended remote, where the individual communicates in real-time with a human registration authority (i.e., RAO).

[5] Refer to the definition of qualified certificates in section 1.6

	○ By Unattended remote, where the communication with the applicant is automated (without involvement of a human Registration Officer (i.e., RAO)).
• S/MIME certificates	**Individual-validated & Sponsor-validated:** • the CA shall authenticate the identity of the Individual according to section 3.2.4 of the Baseline Requirements for S/MIME.

3.2.4 Non-verified Subscriber Information

All information included in the DN shall be checked and authenticated by the TSP RA.

3.2.5 Validation of Authority

The organization's authorized representative shall nominate a certificate requester from the organization who undergoes the certificate request process with the TSP RA. The Authorization of certificate requester is performed as follows with:

1. The TSP RA shall receive a legible copy of a valid government-issued photo ID for the certificate requester, in addition to an official documents demonstrating that the legal entity acts as the requester's employer or that there is a legally binding agreement between them,
2. The TSP RA receives a completed and signed certificate request form from the requestor. The form is signed by the authorized representative, that attests the authority of the requestor,
3. The TSP RA verifies the authority of the authorized representative through an authoritative source or an approved formal communication with the organization,
4. The TSP RA validates the identity of certificate Requester through an in-person identity verification of the Requester against his/her government government-issued ID Card. The ID card (not a copy) shall be presented by the Requester.

For EV TLS & EV Code Signing certificates, TSPs shall conduct additional verifications related validation of Authority according to the EV guidelines and CS BR.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Identification and authentication for re-keying shall be performed as in initial registration.

3.3.2 Identification and Authentication for Re-key after Revocation

Identification and authentication procedures for re-key after revocation shall be same as during initial certification. This follows the conclusion of relevant analysis and investigations by the TSP.

3.4 Identification and Authentication for Revocation Request

The TSP RA shall enforce identification and authentication for revocation requests.

The TSP RA shall validate the revocation request and the identity of the revocation request applicant.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Certificate application for Subordinate CA shall be limited to the certificate types defined in the present CP. The subscriber community for such TSP shall be limited to a user base that the TSP is authorize to service by law

Further details and restrictions shall be specified in the applicable TSP CPS.

4.1.2 Enrollment Process and Responsibilities

For any requested certificate, the subscriber shall ratify a dedicated subscriber agreement.

Further details on the enrolment process shall be specified in the applicable TSP CPS.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Detailed vetting procedures shall be documented as part of the overall certificate application in the applicable TSP CPS. The TSPs' vetting procedures shall conform with the following requirements:

1. General requirements for all certificate applications:
    a. The RA shall assign a unique ID to each certificate application record,
    b. The RA shall store all activities (e-mail communication, phone calls, vetting evidence) along with the certificate application record,
    c. The RA shall maintain its own internal blacklist of entities from which it will not accept certificate requests. The RA logs in this database previously rejected certificate requests due any to suspected or fraudulent usage and revoked certificate requests from entities. This internal blacklist database is queried by the RA whenever it receives any certificate request. If the applicant is in the blacklist, the certification application is rejected
    d. For each certificate type, any malicious certificate or revocation request or a request that fails multiple (more than 3) times shall be added to a blacklist maintained by the RA,
    e. The applicant shall sign or ratify a dedicated subscriber agreement except if the Subordinate CA issues the certificates for itself or for an Affiliate RA, in which case a Terms of Use agreement must be signed.
2. Requirements specific to applicant/certificate type:
    a. For natural person certificates:
        i. The RA shall validate the applicant's identity as described in section 3.2.3, In case of negative outcome, the verification procedure stops, otherwise, the vetting procedure continues,
        ii. The RA shall validate the Linkage between the identity of the Subject of the certificate and a legal person (organization, corporation) identity

when the subject is a natural person who is identified in association with a legal person,

b. For eSeal/Code Signing certificates

i. The RA validates the organization's identity as described in section 3.2.2. In case of negative outcome, the verification procedure stops, otherwise, the vetting procedure continues,

ii. Establish government entity authorized representative as described in section 3.2.2,

iii. Identify authorized certificate requestor as specified in section 3.2.5.

c. For S/MIME:

i. Organization-validated:

i. The RA shall validate the organization's identity, authorized representatives and certificate requestor as mentioned in point (b) above,

ii. The RA shall verify the control of the mailbox address to be included in certificate according to 3.2.2.3.

iii. Sponsor-validated:

i. The RA shall validate the organization's identity as stated in 3.2.2

ii. The RA shall validate the Individual's identity as stated in 3.2.3.2

iii. The RA shall verify the control of the mailbox address to be included in certificate according to 3.2.2.3.

iv. Individual-validated:

i. The RA shall validate the Individual's identity as stated in 3.2.3.2

ii. The RA shall verify the control of the mailbox address to be included in certificate according to 3.2.2.3.

v. Mailbox-validated:

i. No identity validation is required.

ii. The RA shall verify the control of the mailbox address to be included in certificate according to 3.2.2.3.

d. For SSL/TLS certificates:

i. The RA shall validate the organization's identity, authorized representatives and certificate requestor as mentioned in point (b) above,

ii. In case of having the wildcard character (*) in the CN or subjectAltName, the following restrictions shall apply:

1. Wildcard SSL Certificates include a wildcard asterisk character as the first character in the Common Name (CN) attribute of the Subject field and or in the SubjectAltName extension.
2. The wildcard asterisk character must not fall within the label immediately to the left of a registry-controlled or public suffix.

3. Certificate issuance is rejected unless the applicant proves its rightful control of the entire Domain Namespace.

iii. The RA shall verify the validity of TLD included in the certificate request,

iv. The RA shall verify for any of the domains to be included in the certificate is a high-profile domain, if yes then the certificate application is rejected,

v. The RA shall check the CAA records for the domain(s) to verify the authority of the CA to issue a TLS certificate for that domain(s),

vi. The RA shall verify ownership of the domain name using any of the approved methods under section 3.2.2.4 of the CA/Browser Forum Baseline Requirements,

vii. The RA shall verify the ownership of the domain name using any of the approved methods under section 3.2.2.5 of the CA/Browser Forum Baseline Requirements.

e. For device authentication certificates:

i. The RA shall validate the organization's identity, authorized representatives and certificate requestor as mentioned in point (b) above,

ii. The RA shall verify the IT system/device and the control by certificate requester as follows:

1. Identify the IT system/device for which certificate(s) shall be issued. The IT system/device must be part of the IT infrastructure of the organization that the requester belongs to,
2. Verify that the requester is a legitimate sponsor or authorized device or system administrator of the device or system for which certificate(s) shall be issued.

4.2.2 Approval or Rejection of Certificate Applications

The certificate application approval shall be contingent to the following:

- Subject and applicant identity verification,
- Proof of possession of private key,
- Proof of ownership of the device, when applicable,
- Proof of association with an organization, when applicable,
- Any other conditions or constraints such as defined in the CPS.

The TSP CPS shall describe further details on the criteria of approval or rejection of applications.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

The TSP CA shall process a certificate issuance as follows:

- Verify that the certificate request initiated from an authorized RA,
- Issue the certificate with required type identified by a Policy OID identified in the TSP CPS. The issued certificate shall include the information provided in the certificate request.

The TSP shall specify further details on the CA actions as part of the applicable TSP CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The TSP CPS shall specify further details on notifications.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The subscriber shall be given a mechanism to verify that the issued certificate contains required information as per the certificate application. The TSP shall define a criterion of declaring certificate acceptance by the subscriber.

The TSP CPS shall specify further details on certificate acceptance.

4.4.2 Publication of the Certificate by the CA

The TSP CA may publish the issued certificates on the TSP public repository as specified in section 2.2.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The subscribers shall adhere to the following obligations:

- Use the private key and corresponding certificate only for their intended usage as per this CP and the applicable TSP CPS,
- Cease using a private key following expiration or revocation of the corresponding certificate,
- Inform the RA, without any delay, in the event of private key compromise.

4.5.2 Relying Party Public Key and Certificate Usage

A party relying on a certificate issued by the TSP CA shall:

- Use software that is compliant with X.509 and applicable IETF PKIX standards to validate the certificate signature and validity period,
- Validate the certificate by using the CRL, or the OCSP validity status information service in accordance with the certificate path validation procedure,
- Trust the certificate only if it has not been revoked and is within the validity period,
- Trust the certificate only for the signing of certificates and CRLs.

4.6 Certificate Renewal

Certificate Renewal is the act of issuing a new certificate with a new validity period while the identifying information and the public key from the old certificate are duplicated in the new certificate. Certificate Renewal shall not be supported.

4.6.1 Circumstance for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Re-Key

Certificate re-key refers to the issuance of a new certificate with a new subject public key for a subject to whom a certificate has previously been issued. Subject attributes and other certified attributes can be updated

4.7.1 Circumstance for Certificate Re-Key

Certificate re-key may happen while the certificate is still active, after it has expired, or after a revocation.

The certificate re-key shall invalidate any existing active certificates of the same type.

4.7.2 Who May Request Certification of a New Public Key

As per the initial certificate issuance.

4.7.3 Processing Certificate Re-Keying Requests

As per the initial certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per the initial certificate issuance.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per the initial certificate issuance.

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per the initial certificate issuance.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per the initial certificate issuance.

4.8 Certificate Modification

This CP does not specify provisions for certificate modification outside the context of certificate re-key, which results in the generation of a new certificate with the same identification information. Refer to section 4.7 for further details.

4.8.1 Circumstance for Certificate Modification

Not applicable.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

SMIME Certificates

The Subordinate CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. The Subordinate CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. The Subordinate CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);

5. The Subordinate CA obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate should not be relied upon.

The Subordinate CA SHOULD revoke a Certificate within 24 hours and SHALL revoke a Certificate within 5 days if one or more of the following occurs:

6. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
7. The Subordinate CA obtains evidence that the Certificate was misused;
8. The Subordinate CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
9. The Subordinate CA is made aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name);
10. The Subordinate CA is made aware of a material change in the information contained in the Certificate;
11. The Subordinate CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's CP and/or CPS;
12. The Subordinate CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;
13. The Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
14. Revocation is required by the CA's CP and/or CPS; or
15. The Subordinate CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Code Signing Certificates

The Subordinate CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and
   does not retroactively grant authorization;
3. The Subordinate CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in
   the Certificate suffered a Key Compromise;

4. The Subordinate CA is made aware of a demonstrated or proven method that can easily compute the
   Subscriber's Private Key based on the Public Key in the Certificate;
5. The Subordinate CA is made aware of a demonstrated or proven method that exposes the Subscriber's
   Private Key to compromise or if there is clear evidence that the specific method used to
   generate the Private Key was flawed; or
6. The Subordinate CA has reasonable assurance that a Certificate was used to sign Suspect Code.

The Subordinate CA SHOULD revoke a certificate within 24 hours and SHALL revoke a Certificate within 5 days if one or more of the following occurs:

7. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
8. The Subordinate CA obtains evidence that the Certificate was misused.
9. The Subordinate CA is made aware that a Subscriber has violated one or more of its material obligations
   under the Subscriber Agreement or Terms of Use.
10. The Subordinate CA is made aware of a material change in the information contained in the Certificate.
11. The Subordinate CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement.
12. The Subordinate CA determines or is made aware that any of the information appearing in the Certificate is inaccurate.
13. The Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or
    terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP
    Repository.
14. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement.

The Subordinate CA MAY delay revocation based on a request from Application Software Suppliers where immediate revocation has a potentially large negative impact to the ecosystem.

Note: Nothing herein prohibits a CA from revoking a Code Signing Certificate prior to these time frames.

SSL/TLS Certificates

The Subordinate CA MAY support revocation of Short-lived Subscriber Certificates. With the exception of Short-lived Subscriber Certificates, the CA SHALL revoke a Certificate within 24 hours and use the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

1. The Subscriber requests in writing, without specifying a CRLreason, that the CA revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. The Subordinate CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
4. The Subordinate CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) (CRLReason #1, keyCompromise);
5. The Subordinate CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).

With the exception of Short-lived Subscriber Certificates, the CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days and use the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

6. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 (CRLReason #4, superseded);
7. The Subordinate CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
8. The Subordinate CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason #9, privilegeWithdrawn);
9. The Subordinate CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);
10. The Subordinate CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);
11. The Subordinate CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
12. The Subordinate CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement (CRLReason #4, superseded);

13. The Subordinate CA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
14. The Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
15. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement for a reason that is not otherwise required to be specified by this section 4.9.1.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or
16. The Subordinate CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise)

Other Subscriber Certificates

The Subordinate CA shall revoke an issued certificate under the following circumstances:

- Upon request from the subscriber or a representative
- Knowing that the information on the certificate is no longer accurate.
- Discovering that the certificate was issued in a manner not materially in accordance with the procedures required by this CP / the applicable TSP CPS
- Determination that the certificate was issued to a subject other than the one named as the subject of the certificate.
- The subscriber has been declared legally incompetent.
- Obtaining evidence that the certificate was misused
- Obtaining or discovering evidence that subscriber's private key, corresponding to the public key certificate, has been compromised or that there is a demonstrated or proven method that exposes the subscriber's private key to compromise.
- Receiving a lawful order from a law enforcement organization in Iraq to revoke a certificate.

This CP does not specify circumstances for revoking an OCSP certificate or other certificates belong to the Subordinate CA itself apart from the compromise of the related key pair, which shall be considered by the TSP as a disaster and treated as such in conformance with its disaster recovery and business continuity procedures.

The following sub-sections focus only on the revocation provisions that apply to end-entity certificates issued by the Subordinate CA.

4.9.2 Who Can Request Revocation

The subscriber shall be able to request the revocation of his/her certificate.

The RA shall be allowed to revoke subscriber certificates. Only authorized revocation requests shall be accepted by the RA.

The TSP CPS shall specify further details on who can request revocation.

4.9.3 Procedure for Revocation Request

The TSP CPS shall specify further details on the revocation procedure.

4.9.4 Revocation Request Grace Period

There should not be a grace period for revocation. However, the TSP may specify a grace period based on further provisions in section 4.91 of the applicable TSP CPS.

4.9.5 Time Within Which CA Must Process the Revocation Request

Certification revocation requests and problem reports shall be processed within 24 hours from their reception.

4.9.6 Revocation Checking Requirement for Relying Parties

Certificate revocation information is offered to relying parties through CRLs published on a publicly available repository and through its OCSP responder.

Relying parties shall use any of these methods while processing a certificate issued by a TSP CA.

4.9.7 CRL Issuance Frequency (If Applicable)

CRLs shall be issued as per Section 2.3 of this CP.

4.9.8 Maximum Latency for CRLs (if applicable)

Not stipulation.

4.9.9 On-Line Revocation/Status Checking Availability

The TSP OCSP responders shall conform to RFC 6960 0 and/or RFC 5019. OCSP responses must either:

1. Be signed by the Subordinate CA that issued the certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose certificate is signed by the Subordinate CA that issued the certificate whose revocation status is being checked.

In the latter case, the OCSP certificate shall contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

The OCSP URL to be queried by relying party organizations shall be referenced in the certificates issued by the TSP CA.

4.9.10 On-Line Revocation Checking Requirements

The TSP OCSP responders shall support the HTTP GET as described in RFC 6960 and/or RFC 5019.

For the status of Subscriber certificates:

1. OCSP responses must have a validity interval greater than or equal to eight hours;
2. OCSP responses must have a validity interval less than or equal to ten days;
3. For OCSP responses with validity intervals less than sixteen hours, then the TSP Subordinate CA updates the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate; and

4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the TSP Subordinate CA shall update the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For Code Signing certificates:

1. OCSP responses shall be updated at least every four days with a maximum validity of ten days.
2. OSCP responses for code signing and timestamp certificates may be available for up to 10 years after the expiration of the certificate.

For Subordinate CA certificates:

1. The TSP shall update information provided via an OCSP Responder
    a. at least every twelve months and
    b. within 24 hours after revoking a Subordinate CA Certificate

The TSP OCSP responders that receive a request for status of a certificate that has not been issued, shall not respond with a "good" status for such Certificates. OCSP responders for CAs which are not Technically Constrained, in line with Section 7.1.5 of the BR, will not respond with a "good" status for such Certificates.

The TSP operations shall monitor the OCSP responders for requests for "unused" serial numbers as part of its security monitoring procedures and any such case will trigger further investigation.

A certificate serial number within an OCSP request is one of the following three options:

1. “assigned” if a certificate with that serial number has been issued by the Subordinate CA, using any current or previous key associated with that CA subject; or
2. “reserved” if a Precertificate [RFC6962] with that serial number has been issued by
    a. the Subordinate CA; or
    b. a Precertificate Signing Certificate [RFC6962] associated with the Subordinate CA; or
3. “unused” if neither of the previous conditions are met.

4.9.11 Other Forms of Revocation Advertisements Available

Not stipulation.

4.9.12 Special Requirements related to Key Compromise

Subordinate CAs and related Registration Authorities are required to employ reasonable methods to notify Subscribers if their Private Key may have been compromised.

This includes cases where new vulnerabilities have been discovered or where the Subordinate CA at their own discretion decides that evidence suggests a possible Key Compromise has taken place.

In cases where the Key Compromise is acknowledged, Subordinate CAs must revoke Subscriber end-entity Certificates and issue and publish a new Certificate Revocation List (CRL) within 24 hours.

4.9.13 Circumstances for Suspension

Certificate suspension shall not be supported.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

CRLs shall be published on a public repository to be available to relying parties through HTTP protocol queries.

OCSP responder exposes an HTTP interface accessible to relying parties.

4.10.2 Service Availability

The TSP shall maintain 24x7 availability of Certificate status services. The TSP shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

The TSP CPS shall specify the conditions for ending the subscriptions from the TSP subscribers.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA Private Keys are never escrowed. A Subordinate CA that offers key escrow services to Subscribers may escrow Subscriber Private Keys. Any Private Keys that are escrowed must be held in at least the same level of security as when the Key Pair was originally created.

S/MIME BR

The TSP may escrow the Subscriber's Private Key as specified in the TSP CPS. The TSP shall notify Subscribers when their Private Keys are escrowed. Escrowed Private Keys shall be stored in encrypted form. The TSP shall protect escrowed Private Keys from

unauthorized disclosure. The TSP shall recover Subscriber Private Keys only under the circumstances permitted within its TSP CPS.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 Facility, Management, and Operational Controls

This section specifies the minimum physical and procedural security controls that need to be implemented by TSPs.

The TSPs shall implement similar security controls to protect the operation of their CA(s) in line with the present document.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

All critical components of the TSP PKI solution shall be housed in Pakistan within a dedicated secure enclave either in a facility owned by TSP or rented from a reliable service provider.

Physical access controls shall protect the infrastructure, management systems and related operational activities of the TSP PKI solution

5.1.2 Physical Access

Physical security controls shall be enforced so that access of unauthorized persons is prevented through at least four tiers of physical security.

Physical security controls include security guard-controlled building access, biometric access, and CCTV monitoring shall protect the CA systems from unauthorized access, these controls are monitored on a 24x7x365 basis. Further, access to the secure enclave where the PKI systems are hosted shall be enabled only if two trusted employees are present to open the enclave's door.

5.1.3 Power And Air Conditioning

The secure enclave shall be equipped with a UPS, heating ventilating and air conditioning (HVAC) sufficient to maintain the computer equipment within the manufacturers' recommended range of operating temperatures and humidity.

5.1.4 Water Exposures

The TSP shall take reasonable precautions to minimize the impact of water exposure on the TSP PKI hosting facility.

5.1.5 Fire Prevention and Protection

The TSP PKI hosting facility shall follow leading practices and applicable safety regulations in Pakistan, monitored 24x7x365 and equipped with fire and heat detection equipment.

5.1.6 Media Storage

Electronic, optical, and other storage media shall be subject to the multi-tiered physical security and shall be protected from accidental damage (water, fire, electromagnetic interference).

Audit and backup storage media shall be stored in a secure fire-proof safe and duplicated and stored in a secure offsite location.

5.1.7 Waste Disposal

All wastepaper and storage media created within the secure facility shall be destroyed before discarding. Paper media shall be shredded using a crosshatch shredder, and magnetic media shall be wiped by de-magnetization, or physically destroyed. HSMs and related key management devices shall be physically destroyed, or securely wiped (zeroized) prior to disposal.

Authorization shall be granted for the destruction or disposable of any media.

5.1.8 Off-Site Backup

System backups must provide sufficient recovery information to allow the recovery from system failure(s).

Backups shall be made on a daily basis and copies shall be transferred to a secure offsite location on a periodic basis.

Facilities used for offsite backup and archives shall have the same level of security as the TSP CA main site.

5.2 Procedural Controls

The TSP CA shall follow personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the CA staff members, and the satisfactory performance of their duties in the field of PKI governance, operations, and service delivery.

5.2.1 Trusted Roles

All members of the staff operating the key management operations, administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position (i.e., trusted operatives).

The TSP shall conduct an annual clearance check and regularly repeat it of all members of staff who are candidates to serve in trusted roles as a due diligence attempt to determine their trustworthiness and competence.

TSP shall ensure that all the Trusted Roles on which the security of the TSP's operation is dependent, shall be clearly identified in the Subordinate CAs CPS document.

Trusted roles include but are not limited to the following:

- **Administrator:** Responsible for configuring and maintaining the CA.
- **Operator:** day-to-day operation of CA systems and system backup and recovery.
- **Security Officer:** overall responsibility for administering the implementation of the CA's security practices.
- **RA Officer:** Authorized to conduct the vetting as part of the certification request processing.
- **Key Manager:** cryptographic key life cycle management functions (e.g., key component custodians).
- **HSM Auditor:** Owning the credentials for retrieving the HSM audit logs.

5.2.2 Number of Persons Required per Task

The TSP shall maintain and enforce rigorous control procedures to ensure the segregation of duties, based on job responsibility, to prevent single trusted personnel to perform sensitive operations.

The most sensitive tasks such as the following require the presence of two or more persons:

- Physical access to the secure enclave where the CA systems are hosted,
- Access to and management of CA cryptographic hardware security module (HSM),
- Validate and authorize the issuance of certificates.

5.2.3 Identification and Authentication for each Role

Before exercising the responsibilities of a trusted role:

- The TSP confirms the identity and history of the employee by carrying out background and security checks
- The TSP issue access credentials to the designated personnel who need to access equipment located in the secure enclave.
- The TSP provide the necessary credentials that allow designated personnel to conduct their functions.

5.2.4 Roles Requiring Separation of Duties

The TSP shall ensure separation of duties among the following work groups:

- Operating personnel (RA officers, PKI Operators, key custodians, Support etc.)
- Administrative personnel (system admins, network admins, HSM admins etc.)
- Security personnel (enforce security measures)
- Audit personnel (review audit logs)

5.3 Personnel Controls

The TSP shall ensure implementation of security controls regarding the duties and performance of the members of the CA staff members.

These security controls shall be documented in an internal policy, yet it shall include the areas below.

5.3.1 Qualifications, Experience, and Clearance Requirements

The TSP ensures that checks are performed to establish the background, qualifications and experience needed to perform within the competence context of the specific job. Such checks include:

1. Verify the Identity of Such Person: Verification of identity MUST be performed through:
   A. Personal (physical) presence of such person before trusted persons who perform human resource or security functions, and
   B. Verification of well-recognized forms of government-issued photo identification; and

2. Verify the Trustworthiness of Such Person: Verification of trustworthiness includes background checks, which address at least the following, or their equivalent:
   A. Criminal convictions for serious crimes,
   B. Misrepresentations by the candidate,
   C. Appropriateness of references, and
   D. Any clearances as deemed appropriate.

5.3.2 Background Check Procedures

The TSP shall make the relevant checks on prospective staff members by means of status reports issued by a competent authority or third-party statements.

5.3.3 Training Requirements

The TSP shall make available relevant technical training for their staff members to perform their functions.

For the staff members performing information verification and vetting (i.e.,RA officers), public key infrastructure topics, authentication and vetting policies and procedures, applicable CP and CPS material and common threats to the information verification process are included.

The required skills and knowledge for validation specialists are tested through an examination on the information verification requirements.

5.3.4 Retraining Frequency and Requirements

The training content is reviewed and amended on a yearly basis to reflect the latest leading practices and the CA systems' configuration changes.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The TSP shall sanction personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems for the purpose of imposing accountability on the TSP CA staff, as it might be appropriate under the circumstances and as per the prevailing HR Policy and Country Law.

5.3.7 Independent Contractor Requirements

Independent contractors and their personnel are subject to the same background checks as the CA staff. The background checks include:

A. Criminal convictions for serious crimes,
B. Misrepresentations by the candidate,
C. Appropriateness of references,
D. Any clearances as deemed appropriate,
E. Privacy protection, and
F. Confidentiality conditions.

5.3.8 Documentation Supplied to Personnel

The TSP shall make available documentation to the CA staff describing their duties and the operational processes they are fulfilling.

5.4 Audit Logging Procedures

Details on the audit logging procedures shall be defined in the TSP CPS.

This CP specifies minimum requirements on audit logging procedures as per the following sections.

5.4.1 Types of Events Recorded

Audit logs shall be generated for all events relating to the security and services of the Subordinate CA systems. The Subordinate CA SHALL make these records available to its Qualified Auditor as proof of the Subordinate CA's compliance with these Requirements.

The CA SHALL record at least the following events:

1. CA certificate and key lifecycle events, including:
    - Key generation, backup, storage, recovery, archival, and destruction;
    - Certificate requests, renewal, and re-key requests, and revocation;
    - Approval and rejection of certificate requests;
    - Cryptographic device lifecycle management events;
    - Generation of Certificate Revocation Lists;
    - Signing of OCSP Responses (as described in Section 4.9 and Section 4.10); and
    - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
    - Certificate requests, renewal, and re-key requests, and revocation;
    - All verification activities stipulated in these Requirements and the Subordinate CA's Certification Practice Statement;
    - Approval and rejection of certificate requests;
    - Issuance of Certificates;
    - Generation of Certificate Revocation Lists; and
    - Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).
3. Security events, including:
    - Successful and unsuccessful PKI system access attempts;
    - PKI and security system actions performed;
    - Security profile changes;
    - Installation, update and removal of software on a Certificate System;
    - System crashes, hardware failures, and other anomalies;
    - Relevant router and firewall activities (as described in Section 5.4.1.1); and
    - Entries to and exits from the CA facility.

Log records MUST include the following elements:

1. Date and time of event;
2. Identity of the person making the journal record; and
3. Description of the event.

The Code Signing Timestamp Authority MUST log the following information and make these records available to its Qualified Auditor as proof of the Timestamp Authority's compliance with these Requirements:

1. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server,
2. History of the timestamp server configuration,
3. Any attempt to delete or modify timestamp logs,
4. Security events, including:
    - Successful and unsuccessful Timestamp Authority access attempts;
    - Timestamp Authority server actions performed;
    - Security profile changes;
    - System crashes and other anomalies; and
    - Relevant router and firewall activities (as described in Section 5.4.1.1); and;
5. Revocation of a timestamp certificate,
6. Major changes to the timestamp server's time, and
    - System startup and shutdown

5.4.1.1 Router and firewall activities logs

Router and firewall activities logged include:

1. Successful and unsuccessful login attempts to routers and firewalls; and

2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and

3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and

4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts

5.4.2 Frequency Of Processing Log

The TSP shall ensure that the designated personnel reviews log files at regular intervals to validate log integrity and ensure timely identification of anomalous events.

Designated personnel shall report and perform follow-up of these events and any issues affecting audit log integrity.

Evidence of audit log reviews, outcome of the review process, and executed remediation actions shall be collected and archived

5.4.3 Retention Period for Audit Log

The TSP CA shall retain the following, for at least two (2) years:

A. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1) after the later occurrence of:
   i. the destruction of the CA Private Key; or
   ii. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the CA field set to true and which share a common Public Key corresponding to the CA Private Key,
B. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1) after the revocation or expiration of the Subscriber Certificate,
C. Any security event records (as set forth in Section 5.4.1) after the event occurred.

While these Requirements set the minimum retention period, the TSP may choose a greater value as more appropriate to be able to investigate possible security or other types of incidents that will require retrospection and examination of past audit log events.

5.4.4 Protection Of Audit Log

Audit logs shall be protected from unauthorized access, modification, and deletion (except when rotating) by using a combination of physical, procedural, and technical security controls.

Audit logs shall be reviewed only by a designated trusted roles, ensuring the integrity, authenticity, and confidentiality of the data remains unaltered.

5.4.5 Audit Log Backup Procedures

The following rules apply for the backup of the TSP CA audit log:

- Backup media are stored locally in the TSP CA main site, in a secure location
- A second copy of the audit log data and files are stored in an offsite location that provides similar physical and environmental security as the main site

5.4.6 Audit Collection System (Internal vs. External)

If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, the TSP shall determine whether to suspend the relevant CA's operations until the problem is fixed.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

The TSP shall perform the risk assessments annually and every time after major changes in the infrastructure to cover the following scope:

The TSP shall perform risk assessments annually and after any major changes to the infrastructure, covering the following scope:

- **Identification of Threats**: Identify potential internal and external threats that could compromise CA systems and assets.
- **Threat Evaluation**: Assess the likelihood and potential impact of identified threats.
- **Residual Risk Review**: Analyze residual risks considering the effectiveness of existing controls.
- **Mitigation Planning**: Define new measures or controls, as necessary, to mitigate residual risks.
- **Management Alignment**: Collaborate with TSP management to develop and implement a plan for the proposed measures or controls.

The TSP shall also conduct regular vulnerability assessments and penetration testing of all CA assets related to certificate issuance, products, and services. These assessments shall focus on internal and external threats that could lead to unauthorized access, tampering, modification, alteration, or destruction of the certificate issuance process.

Furthermore, the TSP shall establish and maintain a patch management process in accordance with the CA/Browser Forum's Network and Certificate System Security Requirements guideline.

5.5 Records Archival

5.5.1 Types of Records Archived

The TSP CA shall archive all audit logs (as set forth in Section 5.4.1) in addition to the following:

A. Documentation related to the security of CA systems, and Delegated Third Party Systems (Ex. RAs), and
B. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

5.5.2 Retention Period for Archive

Archived audit logs (as set forth in Section 5.5.1) shall be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

Additionally, the TSP CA shall retain, for at least two (2) years:

A. All archived documentation related to the security of CA Systems and Delegated Third Party Systems (as set forth in Section 5.5.1),
B. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of:

i. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates, or
ii. the expiration of the Subscriber Certificates relying upon such records and documentation.

While these Requirements set the minimum retention period, the TSP may choose a greater value as more appropriate in order to be able to investigate possible security or other types of incidents that will require retrospection and examination of past records archived.

5.5.3 Protection of Archive

Records shall be archived in such a way that they cannot be deleted or destroyed. Controls shall be in place to ensure that only authorized personnel are able to manage the archive without modifying integrity, authenticity and confidentiality of the contained records.

5.5.4 Archive Backup Procedures

The TSP CPS or related documentation shall provide details on how archive records are backed up.

5.5.5 Requirements for Timestamping of Records

All recorded events by the TSP CA shall include the date and time of when the event took place, based on the time of the operating system.

The TSP CPS shall specify further details including the controls in place to ensure that all CA systems rely on and are synchronized with a reliable time source.

5.5.6 Archive Collection System (Internal or External)

Only authorized and authenticated personnel shall be allowed to handle archived material.

5.5.7 Procedures to Obtain and Verify Archive Information

Only TSP staff members with a clear hierarchical control and a definite job description may obtain and verify archived information. The TSP shall retain records in electronic or paper-based format.

5.6 Key Changeover

The TSP may periodically changeover its CA keys.

Private keys may be maintained until such time as all relying certificates have expired.

5.7 Compromise And Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The TSP shall specify applicable incident, compromise reporting and handling procedures as part of its business continuity and disaster recovery plan.

The TSP shall specify the recovery procedures used when computing resources, software, and/or data are corrupted or suspected of being corrupted.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

The TSP and all other PKI Participants (other than Subscribers and Relying Parties) shall establish the necessary measures to ensure full recovery of the TSP CA services in case of a disaster, and corrupted servers, software, or data.

The TSP shall implement:

- Disaster recovery solution in a location sufficiently distant from the CA main site,
- Reliable communication between the two sites (for data replication etc.),
- Disaster recovery infrastructure and procedures shall be fully tested at least once a year.

5.7.3 Entity Private Key Compromise Procedures

If the TSP suspects that its CA Private Key is compromised or lost then the TSP shall follow its Incident Response Plan and take appropriate action.

In the event of a key compromise, loss, destruction, or suspected compromise of a TSP CA, the TSP shall take at least the following actions:

- The ECAC PMA shall be notified as soon as there is an indication of suspected compromise.
- The TSP shall work together with the ECAC PMA on deciding whether to continue TSP CA activities or cease operations. If it is decided to revoke the TSP CA certificate:
    - The subscribers holding active end-entity certificates shall be notified by the TSP. The TSP may use the following methodes:
        - An email will be sent to all Subscribers with valid certificates to their registered email address. And/or
        - A notice will be posted on the TSP public repository
    - Publish a TSP CA compromise notice in the TSP's public repository to notify relevant relying parties.
    - All valid end-entity certificates shall be revoked.
    - Last CRL shall be issued
- The ECAC PMA shall decide with the TSP whether a new certificate is going to be issued to the TSP CA.

5.7.4 Business Continuity Capabilities after a Disaster

The TSP shall establish the necessary measures to ensure full recovery of the CA services in case of a disaster, corrupted servers, software or data. These measures shall be specified in the TSP business continuity and disaster recovery plan, to be implemented to ensure business continuity following a natural or other disaster.

The TSP business continuity and disaster recovery plan shall define at least the following:

- Conditions for activating the plan
- Fall-back and resumption procedures
- The responsibilities of the individuals involved in the plan execution
- Recovery time objective (RTO)

- Recovery procedures
- The plan to maintain or restore the business operations in a timely manner following interruption to or failure of critical business processes
- Key termination plan (in case of TSP CA key compromise)
- Procedures for securing the main facility to the extent possible during the period following a disaster and up to recovery of operations in a secure environment in either the main, or secondary site.

5.8 CA or RA Termination

If the TSP and/or the ECAC PMA determine that termination of the TSP CA services is deemed necessary, the TSP shall initiate a termination plan that should have been agreed with the ECAC PMA as part of the TSP onboarding.

The TSP Termination Plan shall cover the below minimum aspects:

a. Provide a written notice to the ECAC PMA of its intention to cease operating its Subordinate CA activities, together with a copy of the TSP's termination plan, at least ninety (90) days before:
   i. the date when it will cease to the Subordinate CA related activities,
   ii. expiry, when applicable, of the TSP authorization for providing its Subordinate CA activities, where the TSP has no intention to apply for an authorization renewal.
b. The TSP arrangement for the retention of archived logs (as set forth in Section 5.5),
c. The TSP arrangement for maintaining the validation status services URLs as mentioned in the certificates that would be valid for the applicable period after termination e.g., Subordinate CAs MAY provide OCSP responses for Code Signing Certificates and Timestamp Certificates for the time period specified in their CPS, which MAY be at least 10 years after the expiration of the certificate.
d. Advertisements about the TSP intention to terminate its Subordinate CA activities within at least sixty (60) days before effective termination or the expiry of its authorization, whichever occurring first, in daily newspapers, or by such other mediums and in the manner the ECAC PMA may determine,
e. Communications towards relevant parties and for transferring archived Subordinate CA records to an appropriate custodian,
f. Plan to assist (as much as possible) the TSP's subscribers with a transition to another TSP,
g. Revoke all certificates, issued by the TSP-CA, that remain unrevoked or unexpired at the end of the notice period, whether the subscribers have requested a revocation.
h. Undertake the necessary measures to ensure that discontinuing its operations does not cause disruption to its subscribers and relying parties.
i. Arrangements to adequately ensure the ongoing maintenance of its systems and security measures for sensitive and accurate data,

j. Addressing any other requirements set forth in the national accreditation framework.

6 Technical Security Controls

This section specifies the minimum key management requirements that need to be implemented by TSPs. The TSPs shall define and follow a security measure to protect their Subordinate CA keys in line with the ECAC Root CP/CPS as well as the present document. Nevertheless, certain distinctions for TSPs are made in the below subsection where applicable for better clarity.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 TSP CAs:

The TSP CA key pairs shall be generated within the memory of an HSM certified as meeting the requirements of section 6.2.11.

The TSP CA Key Generation Ceremony shall be video recorded and stored securely for auditing purposes.

The TSP-CA Key Generation Ceremony shall be witnessed by an internal and external auditor to produce a report or opinion. This is particularly required when the Subordinate CA is not the operator of the Root CA or an Affiliate of the Root CA. The report attests that the TSP:

- Documented its CA key generation and protection procedures in compliance with the present document and the applicable CPS,
- Included appropriate detail in its CA Key Generation Script,
- Executed in the presence of a quorum of authorized personnel including representatives from the ECAC PMA,
- Maintained effective controls to provide reasonable assurance that the CA key pair was generated and protected in conformity with the procedures described in the present document and the applicable CPS,
- Performed, during the CA key generation process, all the procedures required by its CA Key Generation Script.

6.1.1.2 Subscribers

Subscribers' key pairs shall be generated by Subscribers with sufficient security maintained during the key generation process and during the delivery of these keys and corresponding certificate to the subscriber. Subscriber keys shall be generated using [FIPS 186] approved methods.

If TSP operates a remote signing service, then Subscribers key pairs shall be generated by the TSP within the memory of an HSM certified as meeting the requirements of section 6.2.11. These key pairs shall be protected by TSP such that Subscribers shall only access their signing private keys after successful multi-factor authentication.

Keys used for Code Signing Certificates must be generated on a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+.

6.1.2 Private Key Delivery to Subscriber

When the TSP generates subject's key pairs (for all certificate type except SSL), the TSP shall perform private key delivery to Subscriber in accordance with section 6.1.2 of the applicable CA/Browser Forum Requirements.

This CP recommends that the subject's key pairs shall be generated within the memory of cryptographic devices conforming to FIPS 140 Level 2 at minimum and shall be delivered to subscribers using secure communication channel.

6.1.3 Public Key Delivery to Certificate Issuer

The TSP CPS shall provide further details on public key delivery to the certificate issuer.

6.1.4 CA Public Key Delivery to Relying Parties

The TSP shall make its Subordinate CA certificates available to Subscribers and Relying Parties by publishing them at the TSP public PKI repository.

The Subordinate CA's public keys will be also made available on the ECAC public repository https://ecac.pki.gov.pk.

6.1.5 Key Sizes

Where applicable, Subscriber keys must be generated in accordance with the CA/Browser Forum Requirements.

Support for Elliptic Curve Cryptography (ECC) keys for code signing certificates is no longer permitted. All code signing certificates must be issued using RSA keys that meet the specified CA/Browser Forum key length and algorithm requirements.

6.1.6 Public Key Parameters Generation and Quality Checking

RSA: The Subordinate CA SHALL confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 2^16 + 1 and 2^256 - 1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89]

ECDSA: The Subordinate CA SHOULD confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

Certificates issued by the Subordinate CA shall contain a key usage bit string in accordance with RFC 5280 and Certificate Profile document.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The TSP shall generate its TSP CA key pairs and store their private keys within an HSM that is certified according to the rating specified in 6.2.11.

6.2.2 Private Key (n out of m) Multi-person Control

With regards to TSP CA private key shared control, the TSP shall implement technical and procedural mechanisms that implement the principles of dual control and split knowledge. These principles guarantee the participation of multiple trusted individuals for performing sensitive operations with TSP CA cryptographic hardware.

The TSP shall ensure it implements the multi-person control using at least "2 out of 3" scheme.

6.2.3 Private Key Escrow

Private keys of the TSP CA must not be escrowed.

6.2.4 Private Key Backup

The TSP CA private keys are backed up, stored and recovered by multiple and appropriately authorized members of the TSP CA related staff serving in trusted roles. More than one member of the TSP CA management shall authorize key backup and shall assign personnel in writing.

A back-up of the generated key material is taken and stored under the same security measures as the primary key material.

6.2.5 Private Key Archival

Not applicable.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The TSP CA key pairs shall only be transferred to another hardware cryptographic token of the same specification as described in 6.2.11 by direct token-to-token copy via trusted path under multi-person control.

At no time shall the TSP CA private key be copied to disk or other media during this operation.

6.2.7 Private Key Storage on Cryptographic Module

6.2.7.1 Private Key Storage on Cryptographic Module Private key storage for CA keys

No further stipulation other than those stated in clauses 6.2.1, 6.2.2, 6.2.4 and 6.2.6.

6.2.7.2 Private key storage for Timestamp Authorities

The TSP shall comply with the provisions of the CS BR (Section 6.2.7) regarding the protection of the Timestamp Authority's private key.

6.2.8 Method of Activating Private Key

6.2.8.1 TSP CAs

The TSP CA private keys shall be activated using the principles of dual control and split knowledge.

The activation procedure shall involve multi-factor authentication of the HSM admins and key custodians.

6.2.8.2 Subscribers

Subscribers are responsible for activating and protecting access to their private key in accordance with the obligations that are presented in the form of a Subscriber Agreement.

6.2.9 Method of Deactivating Private Key

6.2.9.1 TSP CAs

The Subordinate CAs' private keys maintained in cryptographic hardware shall be deactivated in situations such as:

- When not in use for a longer period,
- The Subordinate CA's HSM storing the Subordinate CA key is operated outside the range of supported temperatures.

Deactivation shall follow documented procedures that ensure the implementation of adequate physical and logical security measures.

6.2.9.2 Subscribers

Activation and deactivation of subscriber's private key depends on the type of certificate and their storage location. This shall be described in the TSP CA CPS and subscriber's agreement.

6.2.10 Method of Destroying Private Key

6.2.10.1 TSP CAs

Destruction of the Subordinate CA keys outside the context of the end of its lifetime shall be authorized by multiple members of the TSP management.

The Subordinate CA keys shall be destroyed through documented procedures involving at least two individuals in trusted roles. These procedures shall enforce the principle of multi-person and split knowledge. The procedures shall also ensure that the Subordinate CA private keys are destroyed by removing permanently from any hardware modules the keys are stored on including backup HSMs.

6.2.10.2 Subscribers

Destruction of subscriber's private key depends on the type of certificate and their storage location. This shall be described in the TSP CA CPS and subscriber's agreement.

6.2.11 Cryptographic Module Rating

The TSP CAs' cryptographic modules shall be certified/validated against [FIPS 140-2] Level 3 or [ISO 15408] Common Criteria (CC) EAL 4+ or above and protection profiles from [CEN EN 419 221] series.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Refer to Section 5.5 for archival conditions.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Subordinate CA key usage and certificate validity shall be set according to below:

	Key Pair Usage Period	Max Validity Period
TSP Subordinate CA	No Stipulation	six (6) years

No Certificate will be issued by the Subordinate CA that is beyond the life of the Subordinate CA itself.

The Subordinate CA shall be rekeyed before approaching the Key Usage Period. The original key shall not be used to sign the certificates but only CRLs and OCSP responder certificates after the Key Usage Period.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.1 TSP CAs

The TSP CAs private keys and HSM activation data is generated during their private key generation ceremonies. Refer to Section 6.1.1 and 6.2.8 of this CP for further details.

6.4.1.2 Subscribers

When the TSP is responsible for the subscribers' key generation, the activation data shall be randomly generated by the CA/RA. This activation data shall be securely delivered to the subscriber.

The TSP is prohibited from generating an SSL key pair on behalf of a subscriber.

6.4.2 Activation Data Protection

The TSP CAs private keys and HSM activation data shall be protected from disclosure by means of cryptographic key material management procedures documented by the TSP in its applicable TSP CPS.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The TSP CAs systems and its operations shall be subject to the following security controls:

- Separation of duties and dual controls for CA operations
- Physical and logical access control enforcement
- Audit of application and security related events
- Continuous monitoring of the CA systems and end-point protection
- Backup and recovery mechanisms for the CA operations
- Hardening of the CA servers' operating system according to leading practices and vendor recommendations
- In-depth network security architecture including perimeter and internal firewalls, web application firewalls, including intrusion detection systems
- Proactive patch management as part of the TSP CA operational processes
- The TSP CA systems enforce multi-factor authentication for all accounts capable of directly causing certificate issuance

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications shall be tested, developed and implemented in accordance with industry best practice development and change management standards.

Purchased hardware or software shall be shipped or delivered in a sealed or shrink-wrapped container and be installed by trained personnel.

6.6.2 Security Management Controls

A formal configuration management methodology shall be used for installation and on-going maintenance of the CA systems.

There shall be a mechanism for detecting unauthorized modification to the CA systems' software or configuration.

The CA software, when first loaded, is checked as being that supplied from the vendor, with no modifications, and is the version intended for use.

6.6.3 Life Cycle Security Controls

Refer to Section 6.6.1 for details.

6.7 Network Security Controls

The TSP shall comply with CAB/Forum Network and Certificate System Security Requirements.

6.8 Timestamping

The Subordinate CA servers' internal clock shall be synchronized with a reliable time source e.g., NTP. The TSP shall provide the details (i.e., frequency, stratum, protocol) in its CPS covering how the Subordinate CA servers' internal clock synchronization is performed.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The TSP shall document the profiles of the certificates its issues in the TSP CA CPS in compliance with the requirement set forth in this section.

7.1.1 Version Number(s)

The TSP CA shall issue X.509 version 3 certificates as defined in RFC 5280.

7.1.2 Certificate Extensions

The Subordinate CA shall issue certificates with X.509 v3 extensions as defined in RFC 5280 in addition to extensions indorsed by the CA/Browser Forum and when applicable profiles described in the ETSI EN 319 412. Section 7.1 of the applicable CPS shall specify details of the contents of the certificates issued by the Subordinate CA.

7.1.3 Algorithm Object Identifiers

X.509 v3 standard OIDs shall be used. The signature algorithms follow the specifications described in sections 6.1.5 and 6.1.6.

7.1.4 Name Forms

As per the naming conventions and constraints listed in section 3.1 of this CP.

7.1.5 Name Constraints

Name constraints are supported as per RFC 5280.

7.1.6 Certificate Policy Object Identifier

In addition to the OIDs indorsed by the ITPC PMA, CA/Browser Forum, the TSP may use its own OID scheme to refer to its CPS and other public documents that it maintains and publishes on its public PKI repository.

7.1.7 Usage of Policy Constraints Extension

Policy Constraints extension shall not be supported.

7.1.8 Policy Qualifiers Syntax and Semantics

The use of policy qualifiers defined in RFC 5280 shall be supported.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificate policies extensions must be processed as per RFC 5280.

7.2 CRL Profile

The Subordinate shall issue the CRLs in accordance with requirements specified in section 7.2 of Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates .

7.2.1 Version Number(S)

The TSP CAs shall support X509 v2 CRLs.

7.2.2 CRL and CRL Entry Extensions

The Subordinate shall issue the CRLs in accordance with requirements specified in section 7.2 of Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates.

7.3 OCSP Profile

The OCSP profile shall comply with the requirements of RFC 6960.

OCSP response signing certificates must the use of the following extensions:

- Key usage (not critical)
- Authority key ID (not critical)
- Extended key usage (critical)
- OCSP no check (not critical)

The TSP shall document further details on the OCSP certificate profile in the applicable CPS.

7.3.1 Version Number(s)

The TSP CA shall support the v1 OCSP responses according to RFC 6960.

7.3.2 OCSP Extensions

No stipulation.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

Based on the types of certificates (certificate usage based on the EKU extension) that the TSP CA can issue, The TSP shall organize an external WebTrust covering applicable criteria to ensure that it meets applicable requirements, standards, procedures, and service levels at least on an annual basis.

The TSP accepts this auditing of its own practices and procedures and makes the audit report publicly available no later than three months after the end of the audit period. The TSP and the ECAC PMA evaluate the results of such audits before further implementing them.

In addition, the ECAC PMA may conduct the compliance verification directly on the TSP or appoint an auditor to do the verification on their behalf to cover other requirements under the national accreditation framework.

8.2 Identity/Qualifications of Assessor

The external WebTrust audits will be performed by qualified auditors that fulfil the following requirements:

- Independence from the subject of the audit
- Ability to conduct an audit that addresses the criteria specified in WebTrust for Certification Authorities
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and third-party attestation function
- Licensed by WebTrust
- Bound by law, government regulation or professional code of ethics
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

External auditors shall be independent third party WebTrust practitioners.

8.4 Topics Covered by Assessment

For WebTrust audits, the types of certificates (certificate usage based on the EKU extension) that the TSP CA can issue determine the combination from the following standards to be covered in the audit:

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities — SSL Baseline with Network Security
- WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL.

- WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements.
- WebTrust Principles and Criteria for Certification Authorities – S/MIME certificates
- WebTrust Principles and Criteria for Certification Authorities – Network Security
- WebTrust Principles and Criteria for Registration Authorities

8.5 Actions Taken as a Result of Deficiency

Issues and findings resulting from an assessment referring to a standard listed in 8.4 shall be reported to the TSP management as well as the ECAC PMA.

The TSP shall develop a remediation plan comprising corrective actions and target resolution dates, which must be shared with the ECAC PMA.

The issues and findings are tracked until resolution by the TSP and ECAC PMA. Additional audits are planned and carried out sufficiently to reach full compliance.

8.6 Communication of Results

The overall results of audits shall be reflected by the ECAC PMA on its public repository.

External audits reports shall be published on the TSP public repository.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The TSP may charge fees for certificate issuance and rekey. Details about the fees shall be documented in the applicable TSP CPS.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation Or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

The TSP shall maintain appropriate insurance to meet its obligations under this CP and will maintain enough insurance coverage for its liabilities to other Participants, including Subscribers and Relying Parties.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The TSP shall consider the following as confidential information:

- Subscriber's personal information that are not part of certificates or CRLs
- Correspondence between and the RA function during the certificate management processing (including the collected subscriber's data)
- Contractual agreements between the TSP and its suppliers
- TSP internal documentation (business processes, operational processes, ….)
- Employees confidential information

9.3.2 Information Not within the Scope of Confidential Information

Any information not defined as confidential by the TSP shall be deemed public. This includes the information published on the TSP's repository.

9.3.3 Responsibility to Protect Confidential Information

The TSP shall protect confidential information through training and policy enforcement with its employees, contractors and suppliers.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The TSP shall observe personal data privacy rules and privacy rules as specified in the present CP. Refer to section 9.4.2 for the scope of private information and to section 9.4.3 for the items that are not considered as private information.

Both private and non-private information can be subject to data privacy rules if the information contains personal data.

Only limited trusted personnel are permitted to access subscriber private information for the purpose of certificate lifecycle management.

The TSP shall not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. When the TSP releases private information, the TSP shall ensure through reasonable means that this information is not used for any purpose apart from the requested purposes. Parties granted access will secure the private data from compromise, and refrain from using it or disclosing it to other third parties. Also, these parties are bound to observe personal data privacy rules in accordance with the relevant laws in the Islamic Republic of Pakistan.

The TSP shall respect all applicable privacy, private information, and where applicable trade secret laws and regulations, as well as its published privacy policy in the collection, use, retention, and disclosure of non-public information.

All communications channels with the TSP/its RA shall preserve the privacy and confidentiality of any exchanged private information. Data encryption shall be used when electronic communication channels are used with the CA systems. This shall include:

- Communications between the RA systems and the subscribers
- Communications between the CA systems and the RA systems.
- Sessions to deliver certificates

9.4.2 Information Treated as Private

All personal information that is not publicly available in the content of a certificate, CRL or OCSP response shall be considered as private information.

9.4.3 Information Not Deemed Private

Information included in the certificate, CRL or OCSP shall not considered as private.

9.4.4 Responsibility to Protect Private Information

The TSP employees, suppliers and contractors handle personal information in strict confidence under the TSP contractual obligations that at least as protective as the terms specified in Section 9.4.1.

9.4.5 Notice and Consent to Use Private Information

The TSP shall ensure that collected personal information is used for the purpose of certificate life cycle management only as consented by the subscribers.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The TSP shall not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. Refer to section 9.4.1 for more details.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

The TSP may own and reserve all intellectual property rights associated with its own databases, web sites, the CAs' digital certificates and any other publication whatsoever originating from the PKI, including this CP.

When the TSP uses software from third party suppliers, it shall ensure that intellectual property rights of the supplier are maintained. This shall be defined in the supplier's license agreement.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The TSP shall warrant that their procedures are implemented in accordance with this CP and the corresponding TSP CPS, and that any certificates issued under the TSP CPS are in accordance with the stipulations specified.

For EV certificates, the TSPs shall adhere to representations and warranties requirements set forth in the EV Guidelines.

9.6.2 RA Representations and Warranties

The TSP shall warrant that it performs RA functions as per the stipulations specified in the TSP CPS.

9.6.3 Subscriber Representations and Warranties

The TSP shall warrant that each subscriber signs a subscriber's agreement with the TSP that lists the subscriber's obligations. The TSP shall use its own CPS to convey legal conditions of usage of certificates to subscribers.

9.6.4 Relying Party Representations and Warranties

The TSP shall use its own CPS to convey conditions of usage of certificates to be honored by relying parties.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers Of Warranties

TSPs may not disclaim any responsibilities or obligations described in this CP. Any such disclaimers of warranties shall be documented in the TSP's CPS and reviewed/validated by the ECAC PMA.

9.8 Limitations of Liability

The total liability of the TSP CAs may be limited provided that TSP operations remain compatible with the provisions of this TSP CP. Such limitations of liability shall be documented in the TSP's CPS and the ECAC PMA.

9.9 Indemnities

No stipulation.

9.10 Term And Termination

9.10.1 Term

The present TSP CP is approved by the ECAC PMA and shall remain in force until amendments are published on the ECAC repository and relevant communication towards TSPs occurred.

9.10.2 Termination

Amendments to this TSP CP are applied and approved by the ECAC PMA and marked by an indicated new version of the document. Upon publishing on the ECAC PMA repository, the newer version becomes effective. The older versions of this CP are archived by on the ECAC repository.

9.10.3 Effect of Termination and Survival

The ECAC PMA coordinates communications towards the TSPs in relation to the termination (and related effects) of this document.

9.11 Individual Notices and Communications with Participants

Notices related to this CP can be addressed to the ECAC PMA contact address as stated in section 1.5.

9.12 Amendments

When changes are required to be done on this CP. The ECAC PMA will incorporate any such change into a new version of this document and, upon approval, publish the new version. The new document will carry a new version number.

9.12.1 Procedure for Amendment

Refer to Section 9.12.

9.12.2 Notification Mechanism and Period

Upon publishing on the ECAC repository, the newer version of the CP becomes effective. The older versions of this document are archived on the ECAC repository.

The ECAC PMA coordinates communication in relation to the amendments of this CP and related effects.

The ECAC PMA reserve the right to amend this CP without notification for amendments that are not material, including without limitation corrections of typographical errors or minor enhancements.

9.12.3 Circumstances under which OID Must Be Changed

Major changes to this CP that may materially change the acceptability of certificates for specific purposes, may require corresponding changes to the OID or qualifier (URL). The ECAC PMA shall coordinate proper communication with relevant parties.

9.13 Dispute Resolution Provisions

The ECAC PMA shall facilitate dispute resolution between PKI participants when conflicts arise as a result of the use of certificates issued under this TSP CP.

9.14 Governing Law

The laws of the Islamic Republic of Pakistan shall govern the enforceability, construction, interpretation, and validity of this CP.

9.15 Compliance with Applicable Law

This CP and provision of TSP CA services are compliant to relevant and applicable laws of the Islamic Republic of Pakistan. In particular:

- Electronic Transaction Ordinance, 2002

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

TSPs complying to the provisions of this TSP CP may not assign their rights, duties or obligations without the prior written consent of the ECAC PMA.

9.16.3 Severability

If any provision of this CP is determined to be invalid or unenforceable, the other sections shall remain in effect until this CP is updated.

In the event of a conflict between the Baseline Requirements and any regulation in Pakistan, the ECAC may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in Pakistan. This applies only to operations or certificate issuances that are subject to that Law. In such event, the ECAC will immediately (and prior to issuing a certificate under the modified requirement) include in this section a detailed reference to the Law requiring a modification of the Baseline Requirements under this section, and the specific modification to the Baseline Requirements implemented by the ECAC. The ECAC will also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CP. Any modification to the ECAC practice enabled under this section will be discontinued if and when the Law no longer applies, or the Baseline Requirements are modified to make it possible to comply with both them and the Law

simultaneously. An appropriate change in practice, modification to this CP and a notice to the CA/Browser Forum, as outlined above, is made within 90 days.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

TSPs shall not be liable for any failure or delay in their performance under the provisions of this TSP CP due to causes that are beyond their reasonable control., including, but not limited to unavailability of interruption or delay in telecommunications services.

9.17 Other Provisions

No stipulation.